# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312052
(43)Date of publication of application : 25.10.2002

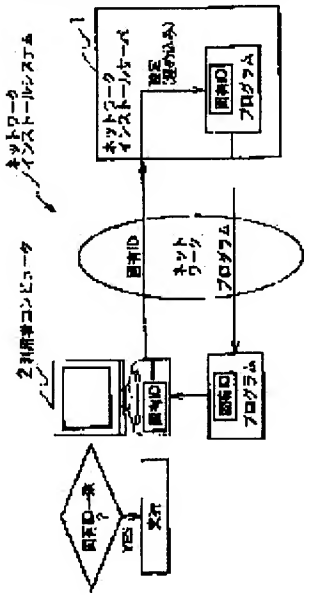
(51)Int.Cl. G06F 1/00
G06F 12/14

(21)Application number : 2001-116025
(22)Date of filing : 13.04.2001

(71)Applicant : NIPPON TELEGRAPH & TELEPHONE WEST CORP
(72)Inventor : YOSHIURA AKIHIKO
IWAKIRI TAKAAKI
SAIKAWA SEIJI
TOKUSA YUKINOBU
INOUE ETSUJI
MIZUMOTO TERUAKI
WATANABE SHUICHIRO
UENO MAYUMI

## (54) COMPUTER PROGRAM, ITS GENERATING METHOD, AND PROVIDING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a computer program from being copied illegally.
SOLUTION: A network install server 1 embeds a physical address, etc., of a specific file acquired from a user computer 2 in the computer program as a proper ID and provides it to the user computer 2. This program reads the proper ID from the user computer 2 and executes the program body only when it is identical to the proper ID embedded.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312052
（P2002－312052A）
(43)公開日　平成14年10月25日(2002.10.25)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード(参考) |
|---|---|---|---|---|
| Ｇ０６Ｆ　1/00 | | Ｇ０６Ｆ　12/14 | ３１０Ｈ | ５Ｂ０１７ |
| 12/14 | ３１０ | | ３２０Ｅ | ５Ｂ０７６ |
| | ３２０ | 9/06 | ６６０Ｆ | |

審査請求　未請求　請求項の数７　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－116025(P2001－116025)

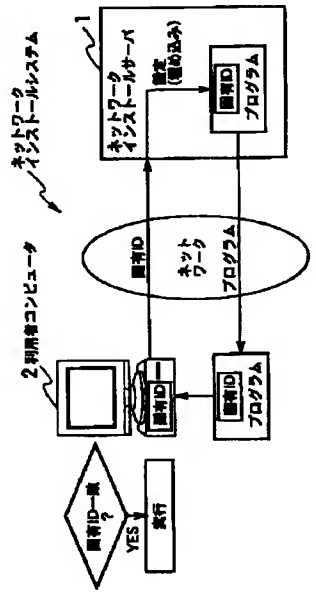
(22)出願日　平成13年４月13日(2001.4.13)

(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番15号
(72)発明者　吉浦　昭彦
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　岩切　高明
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外４名）

最終頁に続く

(54)【発明の名称】　コンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法

(57)【要約】
【課題】　コンピュータプログラムの不正コピーを防止する。
【解決手段】　ネットワークインストールサーバ１は、利用者コンピュータ２から取得した特定ファイルの物理アドレス等を固有ＩＤとしてコンピュータプログラムに埋め込み利用者コンピュータ２に提供する。このプログラムは、利用者コンピュータ２から固有ＩＤを読み出し、埋め込まれた固有ＩＤと一致したときに限って、プログラム本体を実行する。



1

【特許請求の範囲】

【請求項１】　コンピュータを特定して実行可能なコンピュータプログラムであって、
コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、
この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、
一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラム。

【請求項２】　前記特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであることを特徴とする請求項１記載のコンピュータプログラム。

【請求項３】　実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、
入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法。

【請求項４】　コンピュータを特定して実行可能なコンピュータプログラムであって、
コンピュータに設けられた通信部品の物理アドレスを読み出し、
この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、
一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラム。

【請求項５】　実行されるコンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、
入手された前記通信部品の物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法。

【請求項６】　コンピュータを特定して実行可能なコンピュータプログラムの提供方法であって、
コンピュータに固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルの物理アドレスと、当該コンピュータに設けられた通信部品の物理アドレスとを通信回線を介して取得し、
実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、
この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供することを特徴とするコンピュータプログラムの提供方法。

【請求項７】　予め前記コンピュータが利用する通信回線に対応する発信者番号通知により該コンピュータを認証することを特徴とする請求項６記載のコンピュータプログラムの提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不正コピーを防止できるコンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法に関する。

【０００２】

【従来の技術】近年さまざまなビジネスのＩＴ化に伴い、顧客へのサービスがコンピュータアプリケーションソフトウェアや電子データによって行われるようになってきた。また、従来からコンピュータのソフトウェアを製造・販売する事業もますます盛んになりつつあるが、一方そのソフトウェアプログラムや電子データはその性質上、コピーが簡単であり、また不正コピー利用防止については利用者に依存する部分が多く、インターネット接続環境の一般普及なども助力し、ネットワーク上で多くの不正コピーが流通するようになっている。

【０００３】

【発明が解決しようとする課題】従来にあっては、不正コピーの防止方法がいくつか存在するが、これには以下の弱点・問題点が内在する。

【０００４】従来にあっては、不正コピー防止のために、正規利用者へのみシリアルナンバーやキーワードなどの保護解除コードの配布をする。このため、別のコンピュータ、あるいは第３者への保護解除コードを教えると無限に不正利用されてしまう。また、配布するプログラムはネットワークやＣＤ－Ｒ，ＣＤ－Ｒ／Ｗによる流通が容易であり、しかも大規模に行うことができる。

【０００５】また、不正コピー防止のために、ネットワークを用いたプロダクトＩＤ（製品番号）をユーザ登録して監視することがある。このため、ネットワーク上で個人認証を行わない限り、正規利用者による登録なのか、不正コピーの登録なのか判別できない。（２重登録

を監視しても、それが正規利用者が再インストールをしたりＰＣを買い換えたりした場合と不正コピーの登録なのかは判別が不可能、通常は２重登録を許可している。）

また、不正コピー防止のために、コピーや解析が不可能なハードウェアキー（パラレルポートドングルやＵＳＢキーなど）を正規利用者へのみ配布することがある。このため、ハードウェアキーのコストが大きいため、販売するソフトウェアプログラムが高価になってしまう。また、ハードウェアキーの故障や紛失についての対策にコストがかかる。（再発行でも実費かそれ以上の負担を正規利用者へ強いることになる。）

このような不正コピーにより、ソフトウェア業者は少なからぬ被害を被っており、また、安易に行える不正コピーによる消費者のモラル低下も懸念されている。

【０００６】そこで本発明は、上記従来の事情に鑑みなされたものであり、その目的とするところは、により、プログラムの不正コピーが防止できるコンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法を提供することにある。

【０００７】

【課題を解決するための手段】上記従来の課題を解決するために、本発明の請求項１にあっては、コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラムをもって解決手段とする。

【０００８】また、本発明の請求項２にあっては、前記特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであることを特徴とする請求項１記載のコンピュータプログラムをもって解決手段とする。

【０００９】また、本発明の請求項３にあっては、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法をもって解決手段とする。

【００１０】また、本発明の請求項４にあっては、コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め



当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラムをもって解決手段とする。

【００１１】また、本発明の請求項５にあっては、実行されるコンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記通信部品の物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法をもって解決手段とする。

【００１２】また、本発明の請求項６にあっては、コンピュータを特定して実行可能なコンピュータプログラムの提供方法であって、コンピュータに固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルの物理アドレスと、当該コンピュータに設けられた通信部品の物理アドレスとを通信回線を介して取得し、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供することを特徴とするコンピュータプログラムの提供方法をもって解決手段とする。

【００１３】また、本発明の請求項７にあっては、予め前記コンピュータが利用する通信回線に対応する発信者番号通知により該コンピュータを認証することを特徴とすることを特徴とする請求項６記載のコンピュータプログラムの提供方法をもって解決手段とする。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本発明の一実施の形態に係るネットワークインストールシステムの構成図である。

【００１５】このシステムにあっては、プログラムを特定のコンピュータ（実施の形態では利用者コンピュータ２という）に限って利用できるようにするために、ネットワークインストールサーバ１が、利用者コンピュータ２に固有の識別情報（固有ＩＤまたはコンピュータ固有ＩＤという）を、利用者コンピュータ２に配布されるプログラムに設定し（プログラム本体に付与し）、ネッ

トワークを介して利用者コンピュータ２へ配布（送信）する。

【００１６】そして、利用者コンピュータ２では、当該プログラムが、利用者コンピュータ２から固有ＩＤを読み出し、この固有ＩＤと自身に埋め込まれた固有ＩＤとが、一致条件を満たせば、プログラム本体の処理を実行するようになっている。

【００１７】なお、利用者コンピュータ２は、コンピュータのみならず、コンピュータの機能を備える装置、例えば、携帯電話やＰＨＳ端末、ホームゲートウェイ装置、インターネット家電を含むものとして位置づける。

【００１８】本実施の形態では、固有ＩＤとして、ハードディスク上における特定ファイルの物理的位置情報とＬＡＮカードのＭＡＣアドレスを用いている。

【００１９】ここで、ネットワークインストールサーバ１や利用者コンピュータ２を説明する前に、発明の概略とベースとなる技術を説明する。

【００２０】コンピュータを特定するということは、認証ができるということにもなる。ネットワーク上の認証ということについては、これまで主にユーザ認証について論じられてきた。ただし、このユーザという概念は、必ずしも現実世界に存在する人物の特定というわけにはいかない。つまり、本当のところ誰だかわからないのである。したがって、物品の収受や金銭のやりとりのような現実世界の行為を適用しようとすると、「ユーザ」を「（実存する）カード番号」に置き換える等することによって、常に現実世界との結びつきを別途行わなければならない。本発明のコンピュータとは物理的な「モノ」であり、現実世界に存在する「モノ」と「ユーザ」の結びつきを作ることができる。インターネット上で提供されるサービスではインターネット上で完結しているものと、現実世界と結合しているものがある。本発明は後者のサービスにおいて有効な解決手段のひとつとなり得るものである。

【００２１】図２は、ハードディスクの物理的なデータ格納方法を示す図である。図３は、物理アドレスを示す図である。

【００２２】例えば、ファイル：「ａｌｐｈａ」がハードディスクに格納される手順は以下の通りである。手順①　「ａｌｐｈａ」の大きさを調べ、格納できるかどうかを確認する。手順②　ハードディスク上の空きクラスタを集める。手順③　「ａｌｐｈａ」を最小クラスタサイズに分割する。手順④　各クラスタの位置へ「ａｌｐｈａ」を格納する。手順⑤　「ａｌｐｈａ」のデータ要素を持っている各クラスタの位置情報をファイル名ａｌｐｈａをマッピングしてデータテーブルに格納する。

【００２３】上記手順の②において、あるファイルにどのクラスタが割り当てられるかについてはコンピュータの使用状況、つまり空き領域が記録媒体上のどこにあるか、それぞれのコンピュータで異なる。これはコンピュータがハードディスクを空いている領域から順番に効率よく使用するからである。例えばデータの中身も内容も同じファイル「ｂｅｔａ」を２台のコンピュータの同じディレクトリ位置（論理的な位置）に格納しても、ハードディスク上の物理的な位置は必ずしも同じにはならないのである。同じになる確率はハードディスクの容量が大きければ大きいほど低くなる。例えば２０ＧＢのハードディスクを２ＫＢのクラスタブロックで使用している場合、同じ物理的位置に格納される確率は、２ＫＢ／２０ＧＢ＝２０００／２０００００００００＝１，０００万分の１となる。厳密には更にクラスタサイズが何ＫＢであるか、サイズ固定であるか可変であるかによって、さらに確率は低くなる。もので、ハードディスクは取り外し交換等が困難であるため、コンピュータの特定が確実に行える。

【００２４】ハードディスク上では空き領域を格納するファイルのサイズ分の空き領域を集めてくる。この空き領域はクラスタサイズというサイズに区画されており、最終的にファイルが格納できる数の区画を用意する。一つのファイル格納のために使用される区画はディスク上で連続しているわけではなく、離散している。ハードディスクは領域を効率よく使用するためにディスクの内側から空いている区画を拾い出して用意するため、内側に近い場所で空いている領域があればそこから割り当てる。

【００２５】ここで、あるファイルの物理アドレスをコンピュータ固有のＩＤとして配布プログラムに埋め込み、動作時に比較することで、そのコンピュータだけで動作するプログラムが可能になるのである。

【００２６】それぞれのプログラムはあるコンピュータの固有ＩＤ（あるファイルのハードディスク物理格納位置情報）を持っており、プログラムの動作を（１）あるファイル（この例では「ａｌｐｈａ」）の物理アドレスを調べる。（２）自分自身に埋め込まれている固有ＩＤと比較する。（３）合致するならば本来動作、合致しなければ動作終了する。

【００２７】こうすることで、このプログラムはある特定のコンピュータ（対価の支払いをしたなどのそのプログラムおよびサービスを受ける資格や権利があるコンピュータ）以外のコンピュータでは動作しないため、不正にコピーして使用することができなくなる。

【００２８】ここで、ハードディスク物理格納位置情報（物理アドレス）を詳しく説明する。

【００２９】図３に示すように、ハードディスク上のあるファイルのアドレス（シリンダＮｏ：ヘッドＮｏ：セクタＮｏもしくはクラスタブロックアドレス）は、以下のようになる。

【００３０】ファイルデータはＯＳ（オペレーティングシステム）のファイルシステムによって割り当てられたクラスタブロックの単位に分割されて保存される。クラ

スタブロックは、ディスク上の物理的な最小単位（セクタ）のまとまりで構成されている。したがって、ファイルの入出力はファイル名（ファイルシステム上の位置）→クラスタブロック位置→物理構造上の位置（シリンダＮｏ：ヘッドＮｏ：セクタＮｏ）で管理されている

あるファイルの物理構造上の位置やクラスタブロック位置はコンピュータのハードディスクのサイズやオペレーションシステムによって異なる。また、新たに追加されたファイルへのディスク領域の割り当ては、空き領域から割り当てられるため、同じハードウェア構成のコンピュータであっても使用している期間や、使用方法によって割り当てられる物理構造上の位置は異なるのである。ただし、そのディスク上のアドレスは唯一無二ではない。仮に２０ＧＢのハードディスクを持つ２台のコンピュータがあるとすれば、あるファイルに同じディスク上のアドレスが割り当てられる確率は、クラスタサイズが２ＫＢの場合、１０００万分の１の確率である。今後のハードディスク容量の増加傾向を考えると、ソフトウェア配布を目的としたコンピュータ特定には十分な数値である。ただし、実際の運用時には故障時などを想定し、次のＭＡＣアドレスをコンピュータ固有のＩＤに付加し、ＯＲ条件で利用することで、さらなる利便性が確保される。

【００３１】ここで、Ｅｔｈｅｍｅｔカード（ＬＡＮカード、ＮＩＣ：Network InterfaceCardともいう）のＭＡＣアドレスについて説明する。

【００３２】ＥｔｈｅｍｅｔカードのＭＡＣアドレスは、６バイトのコードで、先頭３バイトがベンダーコード、残り３バイトがベンダー内で重複しないよう管理しているコードであるため、世界中で唯一無二のコードである。（コードパターンは２８１兆４７４９億７６７１万０６５６通り）抜き差しがある程度自由なものもあるため、実運用時にはハードディスクの故障やコンピュータの買い替えなどを想定し、ＯＲ条件で併用することで、コンピュータの特定をサポートすることができる。

【００３３】次に、図４を参照して、クラスタブロックの不確定性に関し説明する。

【００３４】ファイルデータはＯＳのファイルシステムによって割り当てられたクラスタブロックの単位に分割されて保存されている。データの読み出しはそのデータを構成するクラスタをすべて集め、つなぎ合わせ、データの書き込みはファイルをクラスタ単位に分割する。

【００３５】ディスク領域はこのクラスタ単位で分割されており、新たにファイルの書き込みが発生した場合は、空いている領域から割り当てられるため、データ消去、書き込みなどを繰り返すうちに、フラグメンテーション（クラスタブロックの不連続）が発生する。フラグメンテーションが多く発生すると、当然ディスクＩ／Ｏのパフォーマンスが低下するが、それを解消するために、データをつなぎ合わせて、アタマから順番に一続きずつ書き込むようにするソフトウェアとして、いわゆるデフラグツールがある。デフラグツールによって、ファイルのディスク上のアドレスは変動するため、流動的で不確定となってしまう場合が考えられる。



【００３６】しかしそのデフラグツールのほとんどが、移動させるファイルの属性を見て、「隠しファイル」「システムファイル」「読取専用ファイル」であれば例外的にファイルの移動をしない。そのため、それらのファイルのディスク上のアドレスは、ディスクをフォーマットしたり、ＯＳを再インストールしない限り変わらない。しかもそのアドレスはコンピュータ毎に異なるものとなる。したがって、あるファイルに隠しファイル・システムファイル・読取専用の属性を与え、さらにそのファイルが格納されたアドレスをファイルに書いておけば、格納位置のアドレスと比較することによってそのファイルがコピーされたか否かを検知できる。

【００３７】次に、ハッシュ値について説明する。

【００３８】ハッシュ値は、ハッシュ関数と呼ばれる１方向の関数によって得られる値、ハッシュ関数一方向であり、得られた値から元の値へ戻すことはできない。（ため、見ても意味がわからない）アルゴリズムにはＭＤ５．ＳＨＡ－１などがある。例えばＭＡＣアドレス００：００：Ｅ２：１１：Ｃ６：Ｃ１をアルゴリズムＳＨＡ－１のハッシュ関数にかけると　Ｅ２Ｃ９４ＤＡ０２２４７１Ｆ７Ｅ８１３Ｆ３２５ＦＦ２Ｄ９４９Ｄ１（大きさ　１２８Ｂｙｔｅｓ）になり、アルゴリズムＭＤ５のハッシュ関数にかけると、５ＢＤ９０ＥＥＣ６２６ＤＤＦＤＥ６０８５２Ｆ１Ａ３ＥＡＣ９ＢＥ３１７７Ｅ７９６３（大きさ　１６０Ｂｙｔｅｓ）になる。

【００３９】例えば、ディスクセクタアドレス０２５５ＣＹＬ－０００ＨＥＤ－０１ＳＥＣをアルゴリズムＳＨＡ－１のハッシュ関数にかけると１１１７０Ａ７３８２３２６５５Ｄ７２Ｆ２６８Ｅ００８８Ｂ３ＣＦＦ（大きさ　１２８Ｂｙｔｅｓ）となり、アルゴリズムＭＤ５のハッシュ関数にかけると、３４Ｃ７２０８９Ａ９９Ｂ８５０３４Ｅ２１Ａ０４Ｂ９Ｂ９４ＤＦ７００Ｅ５３３７３５（大きさ　１６０Ｂｙｔｅｓ）となる。

【００４０】ハッシュ値の元の値はコンピュータ固有のものであり、ハッシュ値はプログラムをインストールするコンピュータ毎に違う値となる。異なるコンピュータでインストールして、プログラムをコピーしても、このハッシュ値が異なるため、インストーラＢ′、プログラム本体は動作しない。またハッシュ値を生成しようとしても、元の値がなにかはハッシュ値をみてもわからない。

【００４１】従って、ハッシュ値を解析しても、固有ＩＤを知ることは殆ど不可能となる。図５は、ネットワークを介したインストール管理のシーケンス図である。図６は、顧客ＤＢ１１に設定されたネットワークインストールの運用条件を示す図である。

【００４２】ネットワークインストールサーバ１は、顧客に関するデータを格納するための顧客ＤＢ１１と、利用者コンピュータ２へ提供するプログラムの本体であるプログラム本体を格納したプログラムＤＢ１２とを備える。これらＤＢ１１，１２はハードディスク等の記憶装置内の記憶領域に構成される。

【００４３】また、プログラム本体に固有ＩＤを埋め込む等の処理を行うプログラム生成部１３を備え、利用者コンピュータ２とプログラム等を交信できるようになっている。プログラム生成部１３はプログラム生成のために予めネットワークインストールサーバ１に記憶された処理プログラムを実行することで実現される。

【００４４】利用者コンピュータ２は、ネットワークインストールサーバ１を利用するために最適化されたプログラムであるネットワークインストーラ２１を備える。ネットワークインストーラ２１は、プログラムＩＤや顧客ＩＤが入力され、所定の操作がなされると、これをネットワークインストールサーバ１へ送信して、プログラムを要求するといった動作を行うようになっている次に、本実施の形態の動作を説明する。

【００４５】図６に示すように、種々の許可を下すための条件が顧客ＤＢ１１に設定される。顧客ＤＢ１１における顧客が利用するプログラム毎のデータ列、具体的には、当該顧客の顧客ＩＤと、当該顧客が購入したプログラムのプログラムＩＤと、購入済みであることを示す「購入」とが設定されたデータ列に、適宜ステータス、コンピュータ固有ＩＤ（ＭＡＣアドレス）、コンピュータ固有ＩＤ（ハードディスクのファイルアドレス）がそれぞれ設定される。

【００４６】インストールを許可するためには、ステータス、コンピュータ固有ＩＤ（ＭＡＣアドレス）、コンピュータ固有ＩＤ（ハードディスクのファイルアドレス）はそれぞれ、値が未設定である必要がある。かかる値がインストール許可条件である。

【００４７】アンインストールを許可するには、ステータスは「インストール」、コンピュータ固有ＩＤ（ＭＡＣアドレス）、コンピュータ固有ＩＤ（ハードディスクのファイルアドレス）のそれぞれに、当該顧客のコンピュータから送信されたＭＡＣアドレス、ハードディスクのファイルアドレスが設定されている必要がある。かかる値がアンインストール許可条件である。

【００４８】なお、ユーザが使用するコンピュータを替えるときのために、再インストールを許可するには、設定された顧客ＩＤと送信された顧客ＩＤとが一致する必要がある。また、ハードディスクの故障時やアンインストール失敗時を想定し、顧客ＩＤまたはプログラムＩＤのどちらかが、利用者コンピュータ２から送信されたものと一致することを条件としてもよい。

【００４９】図５に示すように、ネットワークインストールサーバ１では、プログラムを購入した顧客の電話番号等の顧客情報から、事前に認証用の顧客ＩＤを生成し、その顧客が購入したプログラムのプログラムＩＤを関連づけて顧客ＤＢ１１へ格納しておく。

【００５０】一方、ネットワークインストールサーバ１からの指令に応じて、利用者コンピュータ２でのプログラムのインストール等を制御するネットワークインストーラ２１が配布され、利用者コンピュータ２に事前にインストールされる。

【００５１】図５に示すように、ネットワークインストーラ２１には、インストールしたいプログラムのプログラムＩＤと顧客ＩＤとを登録しておく。

【００５２】先ずネットワークインストーラ２１は、利用者コンピュータ２内を走査し、特定のファイル（読取専用・システム・隠しファイル属性をもつものに限る。これ以降、「ファイルＦ１」と呼ぶ）のハードディスク上のアドレスを固有ＩＤとして取得する。また、ネットワークインストーラ２１は、利用者コンピュータ２を走査し、ＬＡＮカードのＭＡＣアドレスを固有ＩＤとして取得する。そして、顧客ＩＤとプログラムＩＤと２つの固有ＩＤとインストール要求とをネットワークインストールサーバ１に送信する（ステップＳ１）。

【００５３】これに対しネットワークインストールサーバ１は、顧客ＩＤとプログラムＩＤを顧客ＤＢ１１に格納されたインストール許可条件を参照してインストールの資格があるかどうか確認する。利用資格がある場合は、ネットワークインストールサーバ１は、送信されたプログラムＩＤを付与されたプログラム（プログラムＡとする）をプログラムＤＢ１２から読み出し、これに対し、送信された固有ＩＤのハッシュ値を動作制限識別情報として埋め込んでプログラムＡ－１を生成し、利用者コンピュータ２へ送信する（ステップＳ３）。

【００５４】送信されたプログラムＡ－１は利用者コンピュータ２に格納され、ネットワークインストーラ２１により自動的に起動される。起動されたプログラムＡ－１は、利用者コンピュータ２内の固有ＩＤとプログラムＡ－１に埋め込まれた固有ＩＤとが一致するかを判定し、一致していれば、インストールが完了した旨をネットワークインストールサーバ１に通知する（ステップＳ５）。なお、ファイルＦ１の物理アドレス同士が一致し、かつＭＡＣアドレス同士が一致する場合に「一致する」という判定結果としても良いし、どちらかが一致する場合に「一致する」という判定結果としても良い。なお、以下においても同様に、適宜判定基準を定め、この判定基準により判定することができる。

【００５５】通知を受けたネットワークインストールサーバ１は、この完了通知を顧客ＤＢ１１及びプログラムＤＢ１２に反映する。つまり、ステータスを「インストール」に設定し、ハードディスクのファイルＦ１の物理アドレスとＭＡＣアドレスを設定する。そして、出荷本数をカウントする処理を行う。

【００５６】一方、利用者コンピュータ２においては、プログラムＡ－１に含まれる本体プログラムＡが、本来実行すべき処理を行う。

【００５７】ここで、上記インストール管理のシーケンスにおけるプログラムの動作をフローチャートを参照して説明する。

【００５８】図７は、固有ＩＤの送信時の処理の流れを示すフローチャート図である。

【００５９】ネットワークインストーラ２１に顧客ＩＤとダウンロードしたいプログラムのプログラムＩＤを入力すると（ステップＳ１０１）、ネットワークインストーラ２１は先ず、利用者コンピュータ２を走査し、ファイルＦ１のハードディスク上のアドレス、つまり固有ＩＤを取得する（ステップＳ１０３）。次に、利用者コンピュータ２を走査し、ＮＩＣ（ＬＡＮカード）のＭＡＣアドレス（固有ＩＤ）を取得する（ステップＳ１０５）。次に、これら固有ＩＤをネットワークインストールサーバ１に送信する（ステップＳ１０７）。

【００６０】これに対しネットワークインストールサーバ１は、顧客ＩＤとプログラムＩＤを顧客ＤＢ１１内で検索し、利用資格があるかどうか確認し、利用資格がある場合は、固有ＩＤを顧客ＤＢ１１に格納する（ステップＳ１０９）。

【００６１】図８は、ネットワーク配布の際の処理の流れを示すフローチャート図である。先ず、プログラム生成部１３は、送信されてきた固有ＩＤをハッシュ関数にかける（ステップＳ１１１）。次に、得られたハッシュ値をプログラムＡに格納してプログラムＡ－１を生成する（ステップＳ１１３）。そして、生成したプログラムＡ－１を利用者コンピュータ２へ送信する（ステップＳ１１５）。

【００６２】図９は、配布後の処理の流れを示すフローチャート図である。ネットワークインストールサーバ１から送信されたネットワークインストーラ２１は先ず、コンピュータを走査して固有ＩＤを取得し、ハッシュ関数にかける（ステップＳ１２１）。次に、得られたハッシュ値とネットワークインストールサーバ１で埋め込まれたハッシュ値と比較する（ステップＳ１２３）。ここで、不一致のときは、エラーを出力して動作を終了する（ステップＳ１２５）。一方、一致のときは、プログラム本体を抽出して動作させる（ステップＳ１２７）。

【００６３】図１０は、完了通知の送信時の処理の流れを示すフローチャート図である。プログラムが正規利用者へ配布された場合にネットワークインストーラ２１は、顧客ＩＤ、コンピュータ固有ＩＤ、プログラムＩＤをネットワークインストールサーバ１へ送信する（ステップＳ１３１）。ネットワークインストールサーバ１は、各ＤＢへＩＤを登録し、インストール状況フラグを変更する（ステップＳ１３３）。

【００６４】次に、ネットワークを介したアンインストール管理を説明する。図１１は、ネットワークを介したアンインストール管理のシーケンス図である。図１１に示すように、ネットワークインストールサーバ１では、プログラムを購入した顧客の固有ＩＤとインストールされているプログラムのプログラムＩＤを顧客ＤＢ１１に事前に登録しておく。



【００６５】ネットワークインストーラ２１がアンインストールオプションで起動されると、利用者コンピュータ２内を走査して固有ＩＤを取得する。そして、ネットワークインストーラ２１は、顧客ＩＤとプログラムＩＤと固有ＩＤとアンインストール要求をネットワークインストールサーバ１に送信する（ステップＳ１１）。

【００６６】これに対しネットワークインストールサーバ１は、顧客ＤＢ１１のアンインストール許可条件を参照して、アンインストールの資格があるかどうか確認する。資格がある場合は、アンインストールコマンドを発行、送信する（ステップＳ１３）。

【００６７】ネットワークインストーラ２１は、アンインストールを開始し、これが正常に終了したらアンインストール完了通知をネットワークインストールサーバ１に送信する（ステップＳ１５）。

【００６８】通知を受けたネットワークインストールサーバ１は、この完了通知を顧客ＤＢ１１及びプログラムＤＢ１２に反映する。すなわち、顧客ＤＢ１１の該当するステータスを「アンインストール」に設定する。

【００６９】次に、発信者番号認証によるアクセスコントロールを付加したときのインストール管理を説明する。図１２は、発信者番号認証によるアクセスコントロールを付加したときのインストール管理のシーケンス図である。図１２に示すように、プログラムを購入した顧客の電話番号をフレッツオフィス網（都道府県毎に設けられたＩＰ網、「地域ＩＰ網」）と顧客ＤＢへ事前に登録し、さらに電話番号等の顧客情報と認証用ユーザ名を関連づけして顧客ＤＢ１１に格納しておく。

【００７０】一方、ネットワークインストーラ２１には、インストールしたいプログラムのプログラムＩＤを登録しておく。

【００７１】先ず、利用者コンピュータ２が利用する電話回線の番号（発信者番号）が地域ＩＰ網のリモートアクセスサーバ（ＲＡＳ）に送信され（ステップＳ２１）、ＲＡＳ内で発信者の認証が行われる。すなわち、登録した電話番号からのみ接続が許可される。なお、かかる通知を発信者番号通知という。

【００７２】接続が許可されると、ネットワークインストーラ２１がユーザ名とパスワードをネットワークインストールサーバ１に送信し（ステップＳ２３）、ネットワークインストールサーバ１がこれに応答する（ステップＳ２５）。これ以降は、図５に示した処理と同様の処理が行われる。

【００７３】なお、発信者番号認証によるアクセスコン

トロールを付加したときのアンインストール管理については、図１３の発信者番号認証によるアクセスコントロールを付加したときのアンインストール管理のシーケンス図に示すように、図１２に示した処理と同様の発信者認証および応答が行われ、その後、図１１に示した処理と同様のアンインストール管理が行われる。

【００７４】本実施の形態では、このように、コンピュータ固有ＩＤによりプログラムの不正コピーが防止される。また、アンインストール管理を行っているため、重複インストールはできない。つまり、アンインストールしなければインストールするためのプログラムは送信されない。

【００７５】なお、上記説明した処理を実行する処理プログラムは、半導体メモリ、磁気ディスク、光ディスク、光磁気ディスク、磁気テープなどのコンピュータ読み取り可能な記録媒体に記録して、この記録媒体をコンピュータシステムに組み込むとともに、この記録媒体に記録されたプログラムをコンピュータシステムにダウンロードまたはインストールし、このプログラムでコンピュータシステムを作動させることにより、プログラム生成方法を実施するプログラム生成装置として機能させることができるのは勿論であり、このような記録媒体を用いることにより、その流通性を高めることができる。

【００７６】また、上記実施の形態では、利用者コンピュータ２を特定する手段としてファイルＦ１の物理アドレスやＬＡＮカードの物理アドレスを利用したが、これらに代えて、ＣＰＵのシリアルナンバーや、ＩＣカードや指紋認証デバイス等のハードウェアの識別情報を利用することができる。

【００７７】以上説明したように、本実施の形態によれば、利用者コンピュータ２を特定して実行可能なプログラムＡ－１は、利用者コンピュータ２に固定された記憶媒体、つまりハードディスク上の特定ファイルＦ１の物理アドレスや利用者コンピュータ２に設けられた通信部品であるＬＡＮカードの物理アドレスを読み出し、この読み出した物理アドレスと予めプログラムＡ－１に設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合にプログラムＡ－１に予め設定されたプログラム本体の処理を実行するので、このプログラムＡ－１は、他のコンピュータでは動作せず、従って、プログラムの不正コピーを防止できる。

【００７８】また、特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであるので、フラグメンテーションが発生したときでも変わらない物理アドレスにより、プログラムの不正コピーを一層確実に防止できる。

【００７９】また、利用者コンピュータ２に固定された記憶媒体上のファイルＦ１の物理アドレスや利用者コンピュータ２に設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物



理アドレスとが一致するときに予め設定された処理を実行するようにしたプログラムＡ－１を生成する際に、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとしてこのプログラムＡ－１に設定するので、他のコンピュータでは動作せず、従って、プログラムの不正コピーを防止できるコンピュータプログラムを生成することができる。

【００８０】また、利用者コンピュータ２を特定して実行可能なコンピュータプログラムＡ－１の提供に際して、利用者コンピュータ２に固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルＦ１の物理アドレスと、利用者コンピュータ２に設けられた通信部品の物理アドレスとを通信回線を介して取得し、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供するコンピュータプログラムの提供方法をネットワークインストールサーバ１が実施するので、かかる方法によっても、プログラムの不正コピーを防止できる。

【００８１】また、地域ＩＰ網のＲＡＳが、予め利用者コンピュータ２が利用する通信回線に対応する発信者番号通知により該コンピュータを認証するので、かかる方法によっても、プログラムの不正コピーをより確実に防止できる。また、発信者番号によって顧客が特定できるので、料金後払いによるプログラムの販売を行えるという付帯効果も得られる。

【００８２】

【発明の効果】以上説明したように、本発明によれば、コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスや、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行するようにしたので、このプログラムを他のコンピュータで実行することができず、従って、プログラムの不正コピーを防止できる。

【００８３】また、本発明によれば、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスや、コンピュータに設けられた通信部品のを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータプログラムの生成に際

し、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定するようにしたので、このプログラムを他のコンピュータで実行することができず、従って、プログラムの不正コピーを防止できる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係るネットワークインストールシステムの構成図である。

【図２】ハードディスクの物理的なデータ格納方法を示す図である。

【図３】物理アドレスを示す図である。

【図４】クラスタブロックの不確定性に関する説明図である。

【図５】ネットワークを介したインストール管理のシーケンス図である。

【図６】顧客ＤＢ１１に設定された運用条件を示す図である。

【図７】固有ＩＤの送信時の処理の流れを示すフローチャート図である。

【図８】ネットワーク配布時の処理の流れを示すフロー＊チャート図である。



【図９】配布後の処理の流れを示すフローチャート図である。

【図１０】完了通知の送信時の処理の流れを示すフローチャート図である。

【図１１】ネットワークを介したアンインストール管理のシーケンス図である。

【図１２】発信者番号認証によるアクセスコントロールを付加したときのインストール管理のシーケンス図である。

【図１３】発信者番号認証によるアクセスコントロールを付加したときのアンインストール管理のシーケンス図である。

【符号の説明】

１　ネットワークインストールサーバ

２　利用者コンピュータ

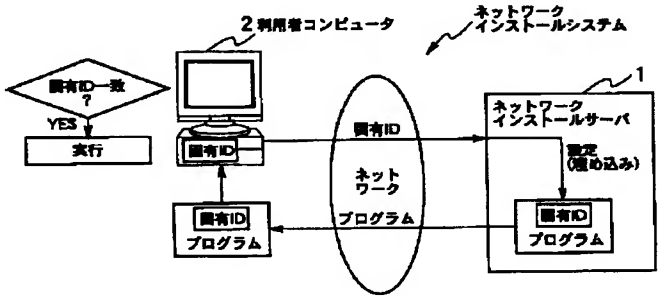
１１　顧客ＤＢ

１２　プログラムＤＢ

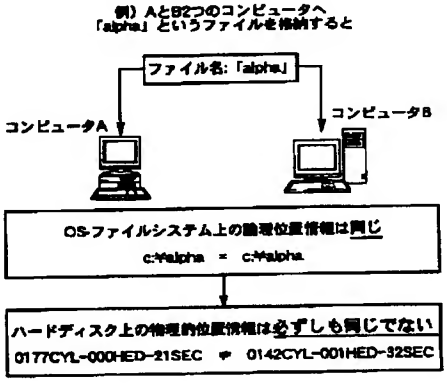
１３　プログラム生成部

２１　ネットワークインストーラ

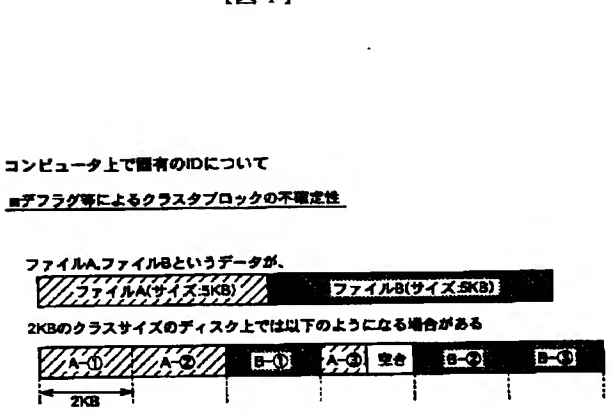
【図１】

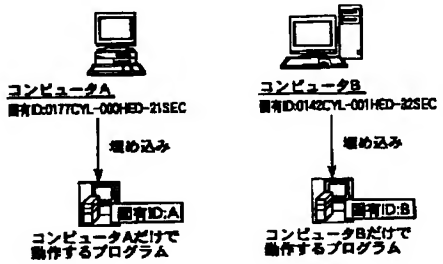



【図２】




【図４】

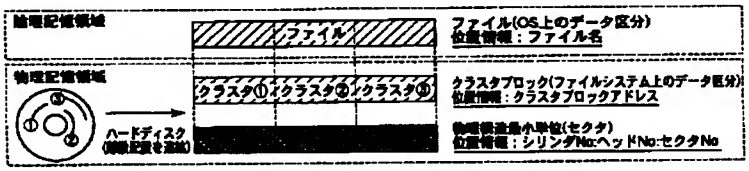


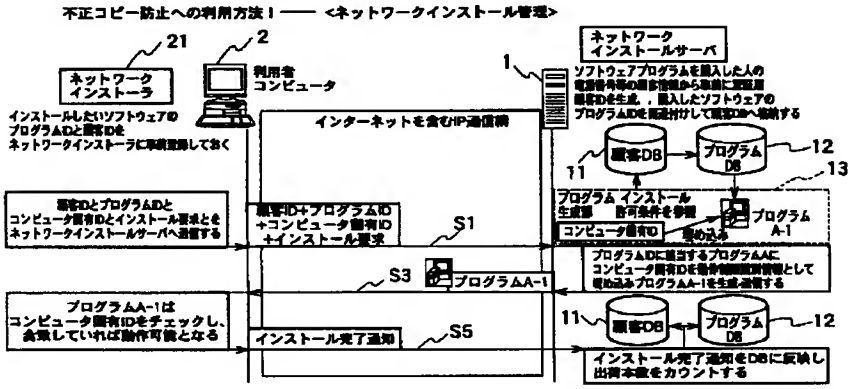
【図３】

コンピュータ上で固有のIDについて

■ハードディスク上のあるファイルの物理アドレス(シリンダNo:ヘッドNo:セクタNoもしくはクラスタブロックアドレス)




【図５】




【図６】

ネットワークインストール運用条件について

インストール許可条件

| 顧客ID | プログラムID | 初期条件 | ステータス | コンピュータ固有ID (MACアドレス) | コンピュータ固有ID (ハードディスク) |
|---|---|---|---|---|---|
| 0001 | A001 | 購入 | - | NULL | NULL |

アンインストール許可条件
※顧客IDとコンピュータID両方とも合致すればアンインストール可

| 顧客ID | プログラムID | 初期条件 | ステータス | コンピュータ固有ID (MACアドレス) | コンピュータ固有ID (ハードディスク) |
|---|---|---|---|---|---|
| 0001 | A001 | 購入 | インストール | 00:00:E2:11:C8:C1 | 0256CYL-000HED-01SEC |

再インストール許可条件(重複インストール防止)
※顧客IDが両方とも合致すれば再インストール可(ただしステータスはアンインストール)

| 顧客ID | プログラムID | 初期条件 | ステータス | コンピュータ固有ID (MACアドレス) | コンピュータ固有ID (ハードディスク) |
|---|---|---|---|---|---|
| 0001 | A001 | 購入 | アンインストール | 00:00:E2:11:C8:C1 | 0256CYL-000HED-01SEC |

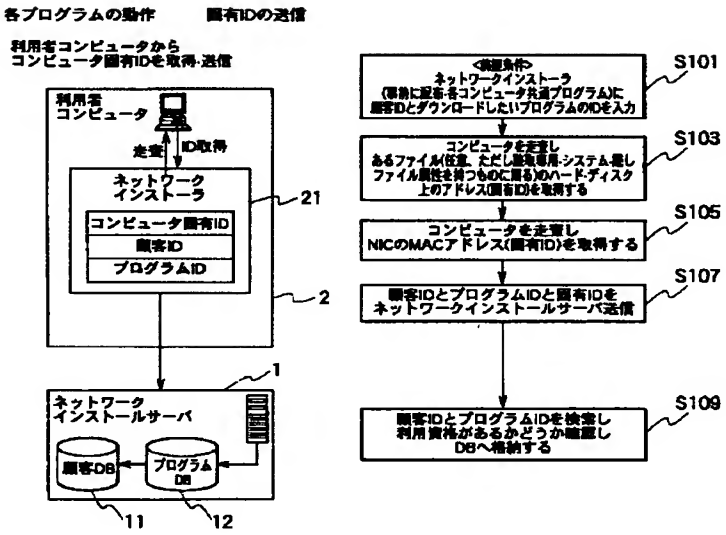
→他のコンピュータへの切り替えが可能

※顧客IDとコンピュータ固有IDのどちらかが合致すれば再インストール可
(ハードディスク故障時やアンインストール失敗時想定)

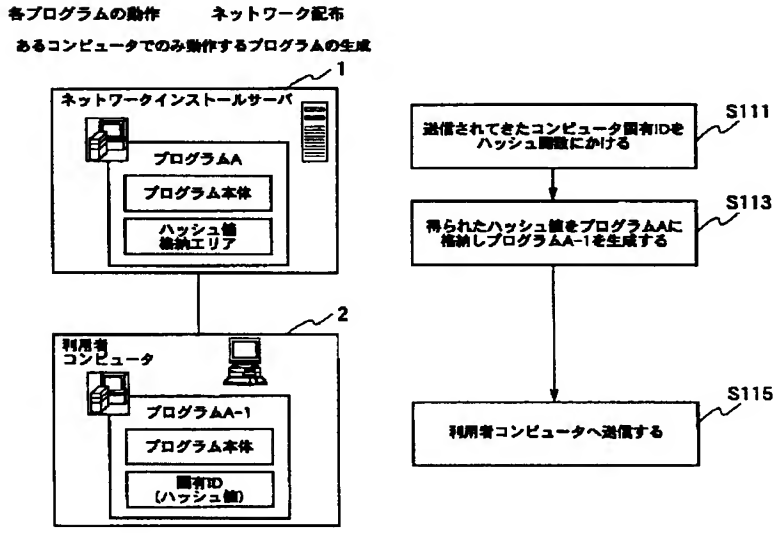
| 顧客ID | プログラムID | 初期条件 | ステータス | コンピュータ固有ID (MACアドレス) | コンピュータ固有ID (ハードディスク) |
|---|---|---|---|---|---|
| 0001 | A001 | 購入 | インストール | 00:00:E2:11:C8:C1 | 0256CYL-000HED-01SEC |

→再インストール後はハードディスクIDを書き換え

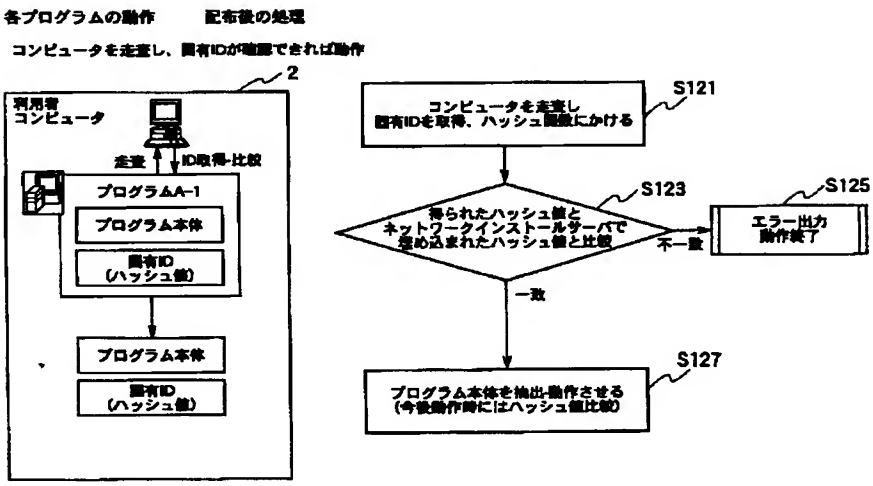
【図７】


各プログラムの動作　　固有IDの送信
利用者コンピュータから
コンピュータ固有IDを取得・送信
利用者
コンピュータ
走査
ID取得
ネットワーク
インストーラ
コンピュータ固有ID
顧客ID
プログラムID
21
2
1
ネットワーク
インストールサーバ
顧客DB
プログラム
DB
11
12
<前提動作>
ネットワークインストーラ
(事前に配布各コンピュータ共通プログラム)に
顧客IDとダウンロードしたいプログラムのIDを入力
S101
コンピュータを走査し
あるファイル(位置、ただし固有用・システム差し
ファイル属性を持つものに限る)のハード・ディスク
上のアドレス(固有ID)を取得する
S103
コンピュータを走査し
NICのMACアドレス(固有ID)を取得する
S105
顧客IDとプログラムIDと固有IDを
ネットワークインストールサーバ送信
S107
顧客IDとプログラムIDを検査し
利用資格があるかどうか確認し
DBへ格納する
S109

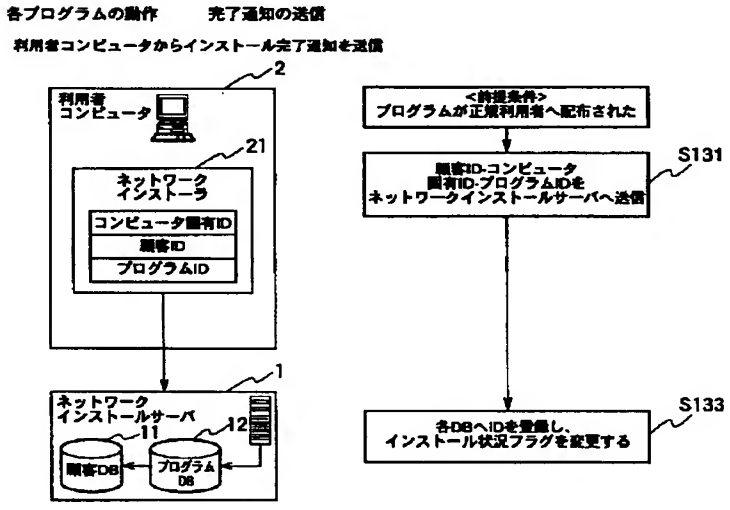
【図８】


各プログラムの動作　　ネットワーク配布
あるコンピュータでのみ動作するプログラムの生成
1
ネットワークインストールサーバ
プログラムA
プログラム本体
ハッシュ値
格納エリア
2
利用者
コンピュータ
プログラムA-1
プログラム本体
固有ID
(ハッシュ値)
送信されてきたコンピュータ固有IDを
ハッシュ関数にかける
S111
得られたハッシュ値をプログラムAに
格納しプログラムA-1を生成する
S113
利用者コンピュータへ送信する
S115

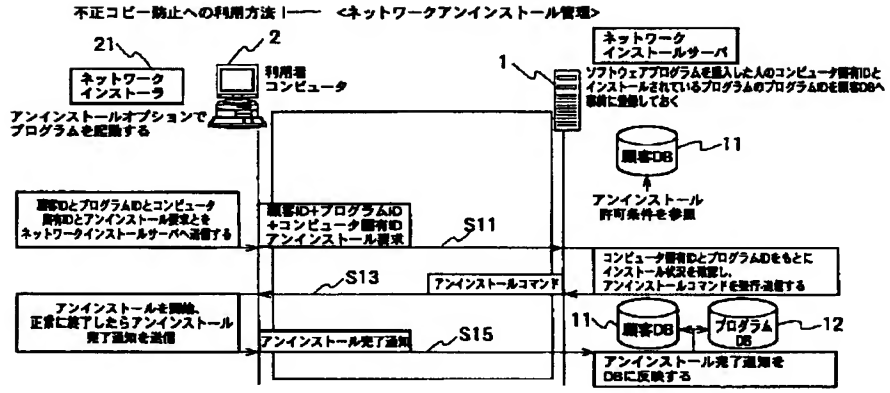
【図９】


各プログラムの動作　　配布後の処理
コンピュータを走査し、固有IDが確認できれば動作
2
利用者
コンピュータ
走査
ID取得-比較
プログラムA-1
プログラム本体
固有ID
(ハッシュ値)
プログラム本体
固有ID
(ハッシュ値)
コンピュータを走査し
固有IDを取得、ハッシュ関数にかける
S121
得られたハッシュ値と
ネットワークインストールサーバで
埋め込まれたハッシュ値と比較
S123
不一致
エラー出力
動作終了
S125
一致
プログラム本体を抽出-動作させる
(今後動作時にはハッシュ値比較)
S127

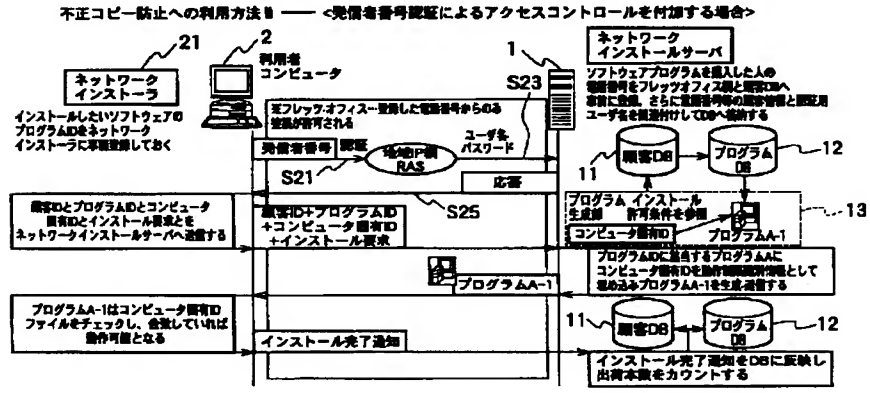
【図１０】


各プログラムの動作　　完了通知の送信
利用者コンピュータからインストール完了通知を送信
2
利用者
コンピュータ
21
ネットワーク
インストーラ
コンピュータ固有ID
顧客ID
プログラムID
1
ネットワーク
インストールサーバ
11
12
顧客DB
プログラム
DB
<前提条件>
プログラムが正規利用者へ配布された
顧客ID-コンピュータ
固有ID-プログラムIDを
ネットワークインストールサーバへ送信
S131
各DBへIDを登録し、
インストール状況フラグを変更する
S133

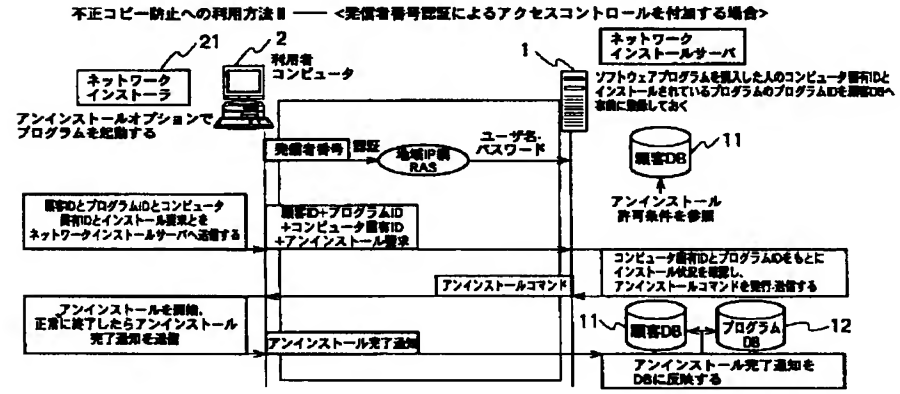
【図１１】


不正コピー防止への利用方法 I ―― <ネットワークアンインストール管理>
21
2
ネットワーク インストーラ
利用者 コンピュータ
1
ネットワーク インストールサーバ
ソフトウェアプログラムを導入した人のコンピュータ固有IDとインストールされているプログラムのプログラムIDを顧客DBへ事前に登録しておく
アンインストールオプションでプログラムを起動する
顧客DB
11
アンインストール許可条件を参照
顧客IDとプログラムIDとコンピュータ固有IDとアンインストール要求とをネットワークインストールサーバへ送信する
顧客ID+プログラムID +コンピュータ固有ID アンインストール要求
S11
コンピュータ固有IDとプログラムIDをもとにインストール状況を確認し、アンインストールコマンドを実行・送信する
S13
アンインストールコマンド
アンインストールを開始、正常に終了したらアンインストール完了通知を送信
アンインストール完了通知
S15
プログラムDB
12
アンインストール完了通知をDBに反映する

【図１２】


不正コピー防止への利用方法 II ―― <発信者番号認証によるアクセスコントロールを付加する場合>
21
2
ネットワーク インストーラ
利用者 コンピュータ
1
ネットワーク インストールサーバ
S23
ソフトウェアプログラムを導入した人の電話番号をフレッツオフィス網と顧客DBへ事前に登録、さらに電話番号等の顧客情報と認証用ユーザ名を関連付けしてDBへ格納する
インストールしたいソフトウェアのプログラムIDをネットワークインストーラに事前登録しておく
定フレッツ・オフィス・登録した電話番号からのみ登録が許可される
発信者番号
認証
地域IP網 RAS
ユーザ名、パスワード
顧客DB
プログラムDB
11
12
S21
応答
S25
プログラム インストール生成部
許可条件を参照
13
顧客IDとプログラムIDとコンピュータ固有IDとインストール要求とをネットワークインストールサーバへ送信する
顧客ID+プログラムID +コンピュータ固有ID +インストール要求
コンピュータ固有ID
プログラムA-1
プログラムIDに該当するプログラムAにコンピュータ固有IDを動作制限許可情報として埋め込みプログラムA-1を生成・送信する
プログラムA-1はコンピュータ固有IDファイルをチェックし、登録していれば動作可能となる
インストール完了通知
インストール完了通知をDBに反映し出荷本数をカウントする

【図１３】


不正コピー防止への利用方法 II ―― <発信者番号認証によるアクセスコントロールを付加する場合>
21
2
ネットワーク インストーラ
利用者 コンピュータ
1
ネットワーク インストールサーバ
ソフトウェアプログラムを導入した人のコンピュータ固有IDとインストールされているプログラムのプログラムIDを顧客DBへ事前に登録しておく
アンインストールオプションでプログラムを起動する
発信者番号
認証
地域IP網 RAS
ユーザ名、パスワード
顧客DB
11
アンインストール許可条件を参照
顧客IDとプログラムIDとコンピュータ固有IDとインストール要求とをネットワークインストールサーバへ送信する
顧客ID+プログラムID +コンピュータ固有ID +アンインストール要求
コンピュータ固有IDとプログラムIDをもとにインストール状況を確認し、アンインストールコマンドを実行・送信する
アンインストールコマンド
アンインストールを開始、正常に終了したらアンインストール完了通知を送信
アンインストール完了通知
プログラムDB
12
アンインストール完了通知をDBに反映する

フロントページの続き

(72)発明者　斉川　清二
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　徳佐　幸展
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　井ノ上　悦司
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　水本　照彰
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　渡辺　修一郎
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　上野　真由美
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内

Ｆターム(参考)　5B017 AA03 AA06 BA01 CA15
5B076 FB06